BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the application of)
)
DAVID WILLIAM HOWELL)
)
Serial No. 10/728,018)
)
Filed 12/03/2003)
)
For TRANSACTION VERIFICATION)

CERTIFICATE OF MAILING VIA EXPRESS MAIL

I hereby certify that the following correspondence was deposited with the United States Postal Service as Regular U.S. Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on December 23, 2003

Barb Foys

Barb Foys, Secy. to Rodney L. Skoglund

TRANSMITTAL SHEET

Enclosed are the following documents:

Submission of Patent Priority Document

Priority Document Patent Application No. 0228384.4

Return Receipt Postcard

AUTHORIZATION TO CHARGE DEPOSIT ACCOUNT

The Commissioner is hereby authorized to charge payment of any fees associated with this communication or credit any overpayment to Deposit Account No. 18-0987.

Respectfully submitted,

Rodney L. Skoglund

Rodney L. Skoglund, Reg. No. 36,010
Renner, Kenner, Greive, Bobak,
Taylor & Weber
First National Tower, 4th Floor
Akron, Ohio 44308
(330) 376-1242

December 23, 2003

GIL.P.US0030

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the application of)
)
DAVID WILLIAM HOWELL)
)
Serial No. 10/728,018)
)
Filed 12/03/2003)
)
For TRANSACTION VERIFICATION)

CERTIFICATE OF MAILING VIA EXPRESS MAIL

I hereby certify that the following correspondence was deposited with the United States Postal Service as Regular U.S. Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on December 23, 2003

Barb Foys

Barb Foys, Secy. to Rodney L. Skoglund

SUBMISSION OF PATENT PRIORITY DOCUMENT

In completion of the requirements for this application, Applicant hereby submits the certified copy of the priority document, U.K. Patent Application No.0228384.4, under 35 U.S.C. § 119.

Should the Office care to discuss this matter in greater detail, the undersigned would welcome a telephone call.

No fee is believed due with the submission of this document.

Respectfully submitted,

Rodney L. Skoglund

Rodney L. Skoglund, Reg. No. 36,010
Renner, Kenner, Grieve, Bobak,
Taylor & Weber
First National Tower, 4th Floor
Akron, Ohio 44308
(330) 376-1242

December 23, 2003

GIL.P.US0030

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 9 December 2003

Patents Form 1/77

Patents Act 1977
(Rule 16)

THE PATENT OFFICE
K
- 4 DEC 2002
RULE 97
NEWPORT

The Patent Office

1/77

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

03DEC02 E768845-5 002915
P01/7700 0.00-0228384.4

1. Your reference

6/LC/P12939.GB

2. Patent application number
(The Patent Office will fill in this part)

0228384.4

04 DEC 2002

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

David William Howell
44 Rochester Drive
Westcliff-on-Sea
Essex SS0 0NL
United Kingdom

Patents ADP number *(if you know it)*

0852106 4001

If the applicant is a corporate body, give the country/state of its incorporation

4. Title of the invention

TRANSACTION VERIFICATION

5. Name of your agent *(if you have one)*

Sanderson & Co.

"Address for service" in the United Kingdom to which all correspondence should be sent *(including postcode)*

34 East Stockwell Street
Colchester
Essex
CO1 1ST

Patents ADP number *(if you know it)*

1446001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.

See note (d))

No

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	12
Claim(s)	5
Abstract	-
Drawing(s)	2 T2

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(Please specify)*	Cover letter

11. I/We request the grant of a patent on the basis of this application.

Sanderson & Co.
Agents for the applicant

Signature

Date
3rd December 2002

12. Name and daytime telephone number of person to contact in the United Kingdom: F.C. Gillam – 01206 571187

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this from, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

TRANSACTION VERIFICATION

This invention relates to apparatus and methods for the verification of transactions to be effected by a card holder having a transaction authorisation card. The invention further relates to a data carrier for use in such a verification procedure.

A large proportion of the population has at least one transaction authorisation card (often called a "credit card"), allowing the card holder to effect purchases. The card allows a vendor to debit an account in the name of the card holder and held at a centralised transaction processing site (CTPS). The card holder then has to settle that account either in one payment by a specified subsequent date or over a period of time with a number of payments, without the vendor being involved. Transaction authorisation cards have become highly popular in view of this ability to pay for purchases over an extended period of time, though not all cards permit this; such cards are usually called "debit cards". A further advantage of credit and debit cards is that they may be used to make purchases other than when the vendor and the purchaser are physically in the same location, for example in a shop. Thus, purchases may be made by mail order, telephone or over the Internet and it is expected that the use of cards for so-called e-commerce will rise very quickly over the coming years.

It is a fact that there is widespread misuse of transaction authorisation cards. Card issuing banks are anxious to cut back on the misuse of cards and take various measures in an attempt to do this but misuse is still increasing. There are proposals for the implementation of new systems in order to effect better checking of transactions as they occur but the difficulty is that this needs

new equipment at each point of sale, new equipment at the CTPS and also new designs of cards able to handle these new proposals. For example, already some cards incorporate a microchip carrying relevant data but few vendors have equipment able to read the microchips. Also, some cards now carry a photograph of the card holder for inspection by a vendor. However, neither of these measures are of any use when a card is being used remotely to effect a transaction, such as by telephone.

The present invention aims at providing relatively simple apparatus and a method which can be used to verify the validity of a transaction as it is being effected by a card holder, and which can be implemented relatively easily, without the need for any new technology directly associated with each card, itself.

According to a first aspect of this invention, there is provided apparatus for the verification of a transaction to be effected by a card holder having a transaction authorisation card, which apparatus comprises:

– a server having stored therein a list, for each card holder intending to use a verification process running on the apparatus, of transaction numbers and for each such transaction number a respective unique code, the server running a programme for comparing the stored codes with a code to be supplied by a card holder on effecting a transaction;

– a local machine whereat a transaction is to be effected which local machine is able to communicate with the server over a data-link;

– a data carrier for use by a card holder and separate from the transaction authorisation card, which data carrier has a list of transaction numbers and the corresponding unique codes for those numbers;

whereby a card holder may effect a transaction at the local machine by using his authorisation card, the card holder also supplying to the local machine a transaction number and the unique code associated therewith for transmission to the server, the server comparing the supplied code with that stored in the server and allows or refuses the transaction dependent upon the result of that comparison.

According to a closely related second aspect of this invention, there is provided a method of verifying a transaction to be undertaken by a card holder having a transaction authorisation card, comprising the steps of:

– programming a server with a list, for each card holder who intends to use the method, of transaction numbers and for each such transaction number a respective unique code;

– providing a card holder with a data carrier having a list of transaction numbers for that card holder and the corresponding unique codes for those numbers which codes are non-sequential on any given carrier;

and then in either order:-

– the card holder effecting a transaction with the card; and

– the card holder being asked to specify a transaction number which number is transmitted to the server, the card holder also being asked for the unique code associated with that transaction number as read from the data carrier, which unique code is transmitted to the server;

– whereafter the server allows or refuses the transaction dependent upon the result of a comparison of the transmitted code with that code programmed into the server.

It will be appreciated that with the apparatus and method of this invention, a card holder is issued with a data carrier which is separate from the card itself though may resemble the card, the data carrier having information on it which must be supplied in order for a transaction to be verified. However, rather than simply carrying a single code, the data carrier has a list of transaction numbers and for each such number, a corresponding unique code, which may be used only once, with a single transaction.

In order to perform the verification method of this invention, a card holder would give the vendor the card if the transaction is being effected in person, or the card number if the transaction is being effected remotely, exactly as is done at the present time. The purchaser then gives the vendor the next unused transaction number from the data carrier and the vendor enters that number into the equipment used to read the card. In this way, the transaction number is transferred back to the CTPS, which responds to the vendor with a request for the purchaser to supply the corresponding unique code. The vendor asks the purchaser to read that unique code from the data carrier and the vendor enters it into the point of sale equipment, for transfer to the CTPS. The CTPS compares the unique code entered by the vendor with that stored in a server at the CTPS, against that particular transaction number for that card holder. If a match is found, then the transaction is verified but if the result of the comparison does not produce a match, then the transaction is refused. However, the verification procedure could be arranged to permit a second attempt in order to allow for misreading of the code from the card, or incorrect entry of the code read out by the purchaser, before final refusal of the intended transaction.

In an alternative and very similar but not preferred verification method, the CTPS does not respond to the vendor by asking for entry of the corresponding unique code for the transaction number given to the vendor by the purchaser. Rather, the purchaser gives the vendor the unique code corresponding to the transaction number previously given and the vendor checks that this unique code corresponds with a code supplied to the vendor by the CTPS. The vendor may perform the comparison and then notify the CTPS accordingly, whereafter the CTPS permits or refuses the transaction.

Yet another alternative is for the CTPS to respond to entry of the card number with a request for a unique code corresponding to the next transaction number as determined by the CTPS. The CTPS will thus transfer to the vendor a request for the unique code for a given transaction number, whereafter the vendor enters the unique code as supplied by the purchaser, on checking the data carrier against the transaction number generated by the CTPS. That unique code is transferred to the CTPS for comparison with the stored code, to permit verification or refusal of the transaction.

If a second "swipe" is taken on a card without the purchaser knowing, or the number of the card is otherwise recorded, that information cannot be used to effect a second, unauthorised transaction, unless the unauthorised person is also in possession of the data card. On attempting to use that information, the unauthorised person would be unable to supply the unique code for the next transaction number on the data card and so the unauthorised purchase would fail. Even if the performance of a verified transaction is entirely monitored by an unauthorised person who thus also is able to record the transaction number and associated unique code, still no further unauthorised purchase can be

made. Though that person could perhaps supply the next transaction number (presuming the card holder makes no intervening further purchase), the unauthorised person still would not be able to provide the unique code for the next transaction number.

Whereas the transaction numbers preferably advance sequentially, it is important that the unique codes do not do so. Each code should be unique for that card holder and should be "random" in the sense that given the previously used code, or even a plurality of previously used codes, the next code cannot be derived from that information. Typically, the codes each should comprise a group of alpha-numeric characters, perhaps of four to six digits in length. The alpha characters preferably are not case-sensitive, in order to facilitate the reading out of the unique code, for example when verifiying a transaction in person or by telephone.

The only way in which fraud still could be committed if the apparatus and method of this invention are implemented is if the transaction card and data carrier together fall into the hands of an unauthorised person. The alternative but not preferred verification procedure mentioned above would be open to abuse if the vendor is in collusion with the unauthorised person and thus confirms the correct supply of the unique code by the purchaser, when in fact that purchaser was unable to supply the code. However, the latter is extremely unlikely since the vendor would not be paid by the CTPS for the transaction, on it becoming apparent that such a fraud had been committed. It is for this reason that the alternative procedure is not the preferred one.

With full implementation of the preferred verification procedure, the only fraudulent transactions possible would therefore be when both a card and data

carrier together are in the possession of an unauthorised person, perhaps by theft – but generally a card holder is able to report theft of a card relatively quickly, so permitting cancellation of the card and preventing continuing fraudulent use.

The individual components of apparatus used in this invention, and also as required for performing the method of this invention, are essentially standard equipment but arranged to run appropriate computer programs to ensure the required functionality. The server may be entirely conventional; the CTPS currently has several such servers running suitable programs and all that is required is a relatively minor modification to that software to ensure the storage of transaction numbers and corresponding unique codes, for each authorised card holder.

It is envisaged that the data carriers would be issued periodically to card holders and have a limited number of transaction numbers together with the corresponding unique codes, suitable for the period between issue dates. Analysis of previous transaction histories, for each user, would show how many transaction numbers should be supplied to a user to ensure that the user has sufficient transaction numbers until issue of the next data carrier. Conveniently, the data carriers might be issued monthly, with a statement in respect of a card holder's account. The system may be arranged in either one of two ways: either the card holder could use a data carrier until all transaction numbers on that carrier have been used, whereafter the card holder moves on to the next supplied carrier, or the data carrier could expire on a given date and then the card holder is required to start using the next supplied carrier. The latter is

preferred, since the data carriers will expire regularly and this will also assist the prevention of fraud, in the event that a carrier has been stolen.

If a card holder believes an unusually large number of transactions will be effected within a given period, such as if the card holder is going on holiday, the card holder may ask the CTPS for a data carrier with more than usual of the predicted number of transaction numbers on it, at the time of effecting payment on a previous account. Alternatively, arrangements may be made to enable a card holder to ask for a further data carrier on a semi-automatic basis, for example by using the technology now available with modern telephones, or over the Internet.

It is important that a card holder ensures that each time a transaction is to be verified, the next available (unused) transaction number is employed. The system could be arranged to prevent verification of a transaction if the same transaction number is used twice, or if a transaction number is skipped, for either of these events might indicate an attempt at fraudulent use. In such a case, the CTPS could call for further checks before verifying a transaction, just as is sometimes employed with the current procedures.

Thus, a further aspect of this invention provides a data carrier for use in a verification procedure for a transaction by a card holder having a transaction authorisation card, which data carrier has a first data area and a second data area, the first data area having a plurality of transaction numbers marked thereon which numbers change incrementally, and the second data area having a plurality of unique codes marked thereon, one such code being associated with each transaction number respectively, whereby for a given transaction number a corresponding unique code may be read off the second data area.

In order to assist a card holder in ensuring that the next transaction number is always employed on seeking verification of a transaction, the card holder could simply strike through a used transaction number at the time it is used, with a suitable writing instrument. However, it is preferred for the unique codes to be covered with a strippable opaque coating, in the manner well known in association with so-called "scratch cards". Then, each time a unique code for a transaction is required, the user would scratch or scrape off the opaque coating of the next unexposed code and read out the code to the vendor. This has the particular advantage that no unused code is visible and so an attempt by a fraudster to read codes from a card whilst it is being used by the proper card holder would be frustrated since no valid code could be read, only previously exposed codes which, following their use, immediately are no longer valid.

In addition to the unique codes being covered with a strippable opaque coating, so too may be the transaction numbers. Thus, this coating would also have to be stripped at the same time as the unique code. Conveniently, therefore, both numbers may be covered by a single coating which is scratched off when a transaction is to be verified. However, the preferred arrangement is for the data carrier to have a simple sequential list of numbers and alongside each a field in which is recorded the unique code for each number, those fields being covered by separate patches of the opaque coating material.

The likelihood of misuse of a data carrier may additionally be reduced, in one of several ways. For example, most card holders already have a personal identification number (PIN) associated with a transaction card. A data carrier could require validation, for example by telephone or over the Internet,

by a user entering the transaction card number followed by a number printed on the data carrier and then by the user's PIN, and only if this sequence of steps is correctly performed, would the data carrier (and so the codes on it), be activated for use. Another possibility would be for a card holder to acknowledge safe receipt of the data carrier on effecting payment on the statement with which the data carrier is supplied to the card holder. It is unlikely that someone wishing to misuse the data carrier, for example following theft of a statement, would make a payment by cheque of at least part of the amount outstanding on the statement in order to acknowledge receipt of the data carrier, since the payment could be traced back to that person.

Though the transaction verification method, apparatus and data carrier of this invention are all apparent from the foregoing, certain further details thereof will now be described though solely by way of example, reference being made to the accompanying drawings, in which:

Figure 1 is a diagrammatic flow chart of a preferred transaction verification sequence; and

Figures 2A and 2B show two possible embodiments of a credit card-sized data carrier for use in this verification sequence.

As mentioned above, the server and point of sale transaction card reader may be essentially conventional in design, construction and general functionality. It is only the programming of that equipment which needs to be revised in order to give the required functionality as hereinbefore specified.

Figure 1 shows a typical verification procedure. In step 1, a purchaser uses a credit card to make a transaction, by supplying the card number to a vendor. The vendor enters that card number into the point of sale equipment in

order to transfer that card number in step 2 to a CTPS, to commence the verification procedure. In step 3, the CTPS responds by asking the vendor to enter on the point of sale equipment the next transaction number which the purchaser intends to use for this procedure. The purchaser uses the data carrier in order to see which is the next transaction number to be employed and informs the vendor; in step 4 that transaction number is transferred to the CTPS. The CTPS responds in step 5 by calling for the unique code which corresponds to that transaction number and the purchaser then uses the data carrier once more, to read off the unique code for the specified transaction number. That unique code is transferred to the CTPS in step 6 and then in step 7, the CTPS verifies the transaction by comparing the supplied unique code with that stored in a server at the CTPS. If the comparison is favourable, the transaction is permitted as shown in step 8, but if the comparison is not favourable then the transaction is refused.

Figures 2A and 2B show typical data carriers for use in the procedure set out above. Figure 2A shows a simple printed card, on an enlarged scale, which gives the name, address and account number (but not the credit card number) for the card holder. If there is no separate account number, then no separate identifying number appears on the data carrier. In column 10, there is a list of transaction numbers and alongside each a unique code for each transaction. As the purchaser uses the data carrier, he may strike through with a pen at least one of the transaction number or unique code, so that it is immediately apparent which is the next transaction number and unique code to employ. The data carrier also includes *valid from* and *valid to* dates and once the *valid*

to date has been reached, then the card holder must start using a replacement data carrier.

In Figure 2B, there is shown a variation of the data carrier of Figure 2A. Here, each of the unique codes is obscured with an opaque coating which may easily be removed by scratching, as with a conventional scratch card. As with the previous example, the transaction numbers are used one at a time but each time a new unique code is required, that code must be exposed. Further, the data carrier of Figure 2B shows that it might, for some verification procedures, be possible to use the transaction numbers out of sequence, so long as only one transaction number is employed at a time.

The reverse of the data carriers shown in Figures 2A and 2B may have continuation transaction numbers and unique codes, if it is expected that a card holder will use more than the number of transaction numbers and codes set out on the front face. In the alternative, advertising material may be carried on the reverse, so helping defray the cost of deploying the verification procedure.

CLAIMS

1. Apparatus for the verification of a transaction to be effected by a card holder having a transaction authorisation card, which apparatus comprises:

– a server having stored therein a list, for each card holder intending to use a verification process running on the apparatus, of transaction numbers and for each such transaction number a respective unique code, the server running a programme for comparing the stored codes with a code to be supplied by a card holder on effecting a transaction;

– a local machine whereat a transaction is to be effected which local machine is able to communicate with the server over a data-link;

– a data carrier for use by a card holder and separate from the transaction authorisation card, which data carrier has a list of transaction numbers and the corresponding unique codes for those numbers;

whereby a card holder may effect a transaction at the local machine by using his authorisation card, the card holder also supplying to the local machine a transaction number and the unique code associated therewith for transmission to the server, the server comparing the supplied code with that stored in the server and allows or refuses the transaction dependent upon the result of that comparison.

2. Apparatus as claimed in claim 1, wherein said local machine comprises a conventional point of sale card reading machine able to communicate with a centralised server.

3. Apparatus as claimed in claim 1 or claim 2, wherein said transaction authorisation card comprises a conventional credit card or debit card.

4. Apparatus as claimed in any of the preceding claims, wherein said data-link comprises a conventional public telephone network service.

5. Apparatus as claimed in claim 4, wherein said data carrier has a first data area and a second data area, the first data area having a plurality of transaction numbers marked thereon which numbers change incrementally, and the second data area having a plurality of unique codes marked thereon, one such code being associated with each transaction number respectively, whereby for a given transaction number a corresponding unique code may be read off the second data area.

6. Apparatus as claimed in claim 5, wherein the unique codes of the data carrier are covered with a strippable opaque coating, whereby each unique code may be exposed by removing the strippable coating therefrom.

7. Apparatus as claimed in claim 6, wherein the transaction numbers of the data carrier and associated with the unique codes are also covered with a strippable opaque coating, whereby the next transaction number and its associated code are together exposed when required for use.

8. A method of verifying a transaction to be undertaken by a card holder having a transaction authorisation card, comprising the steps of:

– programming a server with a list, for each card holder who intends to use the method, of transaction numbers and for each such transaction number a respective unique code;

– providing a card holder with a data carrier having a list of transaction numbers for that card holder and the corresponding unique codes for those numbers which codes are non-sequential on any given carrier;

and then in either order:-

– the card holder effecting a transaction with the card; and

– the card holder being asked to specify a transaction number which number is transmitted to the server, the card holder also being asked for the unique code associated with that transaction number as read from the data carrier, which unique code is transmitted to the server;

– whereafter the server allows or refuses the transaction dependent upon the result of a comparison of the transmitted code with that code programmed into the server.

9. A method as claimed in claim 8, in which the data carrier is valid for a limited period and is replaced periodically with a fresh supply of transaction numbers and corresponding unique codes.

10. A method as claimed in claim 8, in which the data carrier is valid for only a specified number of transactions and is replaced with a fresh supply of transaction numbers and corresponding unique codes when that specified number of transactions has been effected.

11. A method as claimed in any of claims 8 to 10, in which the data carrier must be activated following receipt thereof by a card holder, before the data carrier may be employed to verify transactions.

12. A method as claimed in any of claims 8 to 11, in which the server permits at least a second attempt at verifying a transaction, in the event that the first attempt results in a refusal of the transaction.

13. A method as claimed in any of claims 8 to 12, in which the server communicates with a vendor having control of a point of sale local machine and the vendor requests the relevant information from the card holder and acts as an intermediary between the card holder and the server.

14. A method as claimed in any of claims 8 to 13, in which the transaction authorisation card comprises one of a credit card or a debit card.

15. A method as claimed in claim 14, in which a fresh data carrier is supplied to the card holder with a statement of transactions effected over a previous period.

16. A modification of the method as claimed in any of claims 8 to 15, in which modification the server generates the transaction number to be used to verify a transaction and returns that transaction number to the card holder so that the card holder may supply the server with the corresponding unique code from the data carrier, for verification.

17. A data carrier for use in a verification procedure for a transaction by a card holder having a transaction authorisation card, which data carrier has a first data area and a second data area, the first data area having a plurality of transaction numbers marked thereon which numbers change incrementally, and the second data area having a plurality of unique codes marked thereon, one such code being associated with each transaction number respectively, whereby for a given transaction number a corresponding unique code may be read off the second data area.

18. A data carrier as claimed in claim 17, wherein the unique codes are covered with a strippable opaque coating, whereby each unique code may be exposed by removing the strippable coating therefrom.

19. A data carrier as claimed in claim 18, wherein the transaction numbers associated with the unique codes are also covered with a strippable opaque coating, whereby the next transaction number and its associated code are together exposed when required for use.

20. Apparatus for the verification of a transaction to be effected by a card holder having a transaction authorisation card and substantially as hereinbefore described with reference to the accompanying drawings.

21. A method of verifying a transaction to be undertaken by a card holder having a transaction authorisation card and substantially as hereinbefore described with reference to Figure 1 of the accompanying drawings.

22. A data carrier for use in a verification procedure for a transaction by a card holder having a transaction authorisation card and substantially as hereinbefore described with reference to and as illustrated in Figures 2A and 2B of the accompanying drawings.

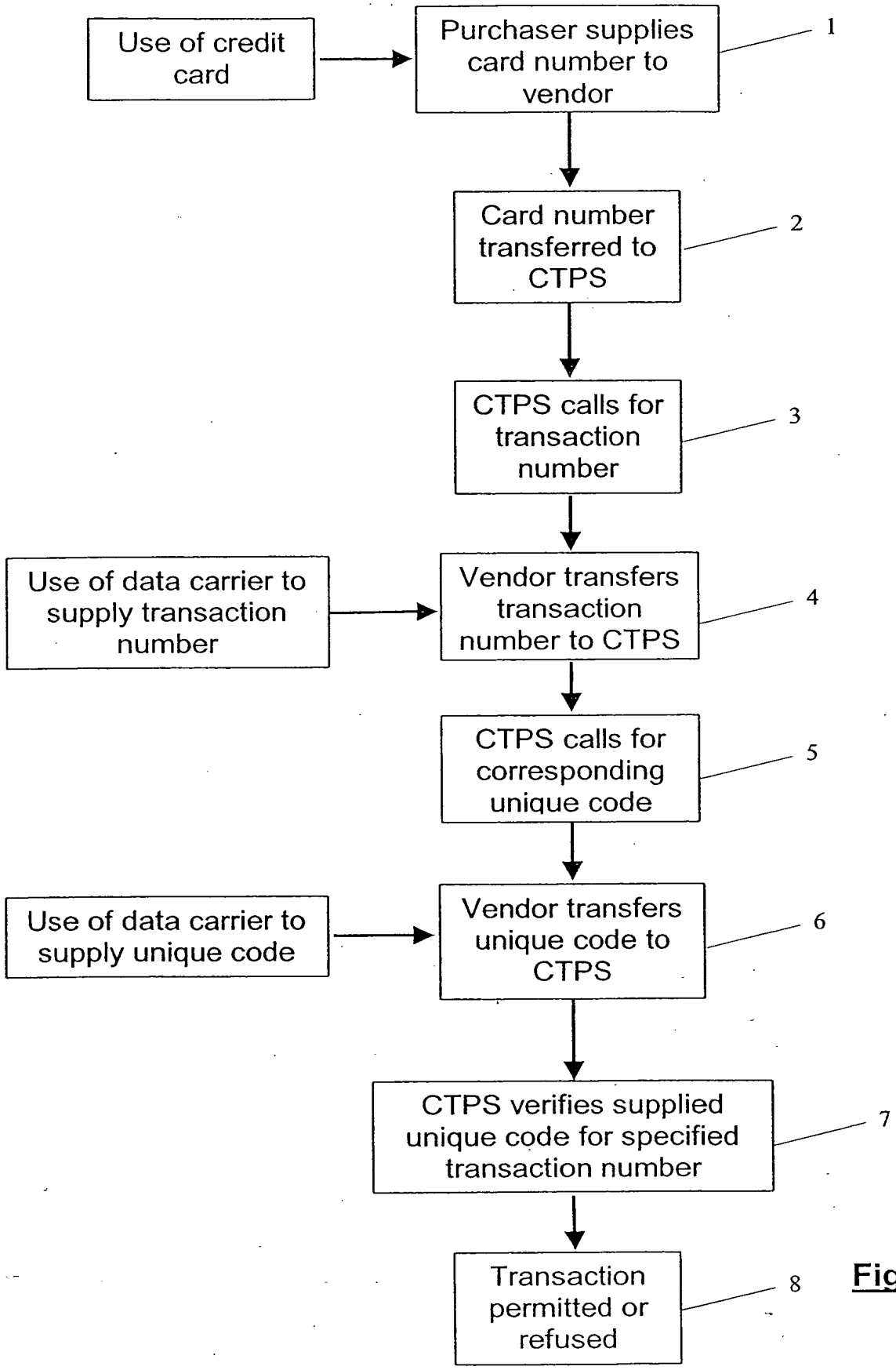
Use of credit card
Purchaser supplies card number to vendor
1
Card number transferred to CTPS
2
CTPS calls for transaction number
3
Use of data carrier to supply transaction number
Vendor transfers transaction number to CTPS
4
CTPS calls for corresponding unique code
5
Use of data carrier to supply unique code
Vendor transfers unique code to CTPS
6
CTPS verifies supplied unique code for specified transaction number
7
Transaction permitted or refused
8

Figure 1

Fig 2A

TRANSACTION CODES

1/1/03 to 1/2/03

Mr Peter Smith
1 Acacia Drive
Romford
Essex RM3 2PP

Account N°
1234567890

Transaction		Code
11	=	11 AMB
12	=	12 OPA
13	=	13 TAX
14	=	14 POL
15	=	15 LTP
16	=	16 PMS
17	=	17 APB
18	=	18 SMZ
19	=	19 PFT
20	=	20 TFO

Fig 2B

TRANSACTION CODES

1/1/03 to 1/2/03

Mr Peter Smith
1 Acacia Drive
Romford
Essex RM3 2PP

Account N°
1234567890

Transaction		Code
~~1~~	=	1 ABC
~~2~~	=	2 PMZ
3	=	[redacted]
4	=	[redacted]
5	=	[redacted]
6	=	[redacted]
~~7~~	=	7 MOT
8	=	[redacted]
9	=	[redacted]
10	=	[redacted]